

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of
A 2015 silver Mercedes Benz, Class C Sedan, bearing
California license plate 8XQZ564 and VIN ending in 88618
(Subject Premises A-2).

Case No. 22-9072 MB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of Arizona:

As further described in Attachment A-2.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

As set forth in Attachment B.


YOU ARE COMMANDED to execute this warrant on or before 4/6/2022 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any United States Magistrate Judge on criminal duty in the District of Arizona.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized ☐ for 30 days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 3/23/2022@6:39 pm



Judge's signature

City and state: Phoenix, Arizona

Honorable EILEEN S. WILLETT, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A-2

PROPERTY TO BE SEARCHED

A 2015 silver Mercedes Benz, Class C Sedan, bearing California license plate 8XQZ564 and VIN ending in 88618 (Subject Premises A-2).



ATTACHMENT B
PROPERTY TO BE SEIZED

Agents are authorized to search for evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 924(a)(1)(A) (False Statement During the Purchase of a Firearm), including:

1. Any firearms including firearms parts, frames, receivers, accessories, magazines, cases, boxes.
2. Any ammunition and components, including bullets, brass, casings, boxes, and cases.
3. Concealed Weapons Permit(s).
4. Records, documents, notes, receipts, ledgers, invoices, indicia, or photographs showing the acquisition or sale of any firearms and firearm parts.
5. Receipts, bank account records, buyer or seller lists, money transfer records, agreements for storage facilities, records of mail service, ledgers, and notebooks showing the acquisition and/or disposition of firearms and firearm parts.
6. Books, records, receipts, notes, ledgers, personal checks and other papers relating to the transportation, ordering, and purchase of firearms, firearm accessories, or ammunition.
7. Ledgers, customer lists, contact lists, inventory lists, vendor lists, or any notes containing the individual names of such persons, telephone numbers or addresses of such persons.
8. Bank documents and records, financial documents and records, and any records and documents relating to any bank or financial transactions, including: correspondence, signature cards and applications for all credit card accounts, investment accounts, and retirement accounts; copies of monthly, quarterly, yearly or periodic account statements; pre-paid credit/debit cards; money wrappers; copies of check journals, check ledgers, checkbooks, check registers, deposit tickets, deposit items, credit memos, debit memos, canceled checks, loan applications, financial statements,

mortgage or promissory notes; copies of loan ledger accounts; copies of annual loan statements; application for bank drafts, cashier's checks, and foreign drafts; and records relating to employment, wages earned and paid, business income earned, and other compensation records.

9. Records indicating occupancy, residency, or rental of the search location, including rental or lease agreements, and keys.
10. Records pertaining to the rental of self-storage units, post office boxes, or mailboxes.
11. Electronic equipment, including cellular telephones, computers, disks, thumb drives, and any media storage device, GPS devices and their memory, and related manuals used to generate, transfer, count, record or store the information described in this Attachment B. For any computer or electronic storage medium whose seizure is otherwise authorized by this warrant, and any computer or electronic storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, the "Electronic Storage Device"), this warrant also authorizes the seizure of the following:
 - a. Evidence of who used, owned, or controlled the Electronic Storage Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, and browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. Call details including call history, duration of calls, text messages, and text message history;
 - c. Electronic correspondence and communications stored on, or accessed through, the Electronic Storage Device relating to the procurement of export-controlled items, to include e-mails and attached files, text messages, any Short Message Service messages (SMS), Instant Messages (IM), Multimedia Message Service messages, or similar text or electronic messages made

through additional applications from which communication can be made, and instant messaging logs;

- d. Contact lists stored on or accessed through the Electronic Storage Device, to include telephone and e-mail contact names, telephone numbers, addresses, and e-mail addresses;
- e. Evidence of software that would allow others to control the Electronic Storage Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- f. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- g. Evidence indicating how and when the Electronic Storage Device was accessed or used to determine the chronological context of Electronic Storage Device access, use, and events relating to the crime under investigation and to the user of the Electronic Storage Device;
- h. Evidence of the attachment to the Electronic Storage Device of other storage devices or similar containers for electronic evidence;
- i. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Electronic Storage Device;
- j. Evidence of the times the Electronic Storage Device was used;
- k. Passwords, encryption keys, and other access devices that may be necessary to access the Electronic Storage Device;
- l. Documentation and manuals that may be necessary to access the Electronic Storage Device or conduct an examination of the Electronic Storage Device;
- m. Any records of or information about Internet Protocol addresses used

- by the Electronic Storage Device;
 - n. Contextual information necessary to understand the evidence described in this Attachment B; and,
 - o. Any peripheral equipment used to facilitate the transmission, creation, display, encoding or storage of records, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners.
12. Items used for identification, including identification cards under fictitious names, and any other type of false identifying documents.

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of
a 2015 silver Mercedes Benz, Class C Sedan, bearing
California license plate 8XQZ564 and VIN ending in 88618
(Subject Premises A-2).

Case No. 22-9072 MB

APPLICATION FOR A SEARCH WARRANT

I, Katherine Rottman, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

As further described in Attachment A-2.

located in the District of Arizona, there is now concealed:

As set forth in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code/Section	Offense Description
18 U.S.C. § 924(a)(1)(A)	False Statement During the Purchase of a Firearm

The application is based on these facts:

See attached Affidavit of ATF Special Agent Katherine Rottman.

☒ Continued on the attached sheet.

☐ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA Coleen Schoch



Telephonically

Sworn to before me and signed in my presence.

Date: 3/23/2022@6:39pm

City and state: Phoenix, Arizona

KATHERINE ROTTMAN Digitally signed by KATHERINE ROTTMAN
Date: 2022.03.23 18:13:53 -07'00'

Applicant's Signature

KATHERINE ROTTMAN, ATF Special Agent

Printed name and title



Judge's signature

Honorable EILEEN S. WILLETT, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A-2

PROPERTY TO BE SEARCHED

A 2015 silver Mercedes Benz, Class C Sedan, bearing California license plate 8XQZ564 and VIN ending in 88618 (Subject Premises A-2).



ATTACHMENT B

PROPERTY TO BE SEIZED

Agents are authorized to search for evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 924(a)(1)(A) (False Statement During the Purchase of a Firearm), including:

1. Any firearms including firearms parts, frames, receivers, accessories, magazines, cases, boxes.
2. Any ammunition and components, including bullets, brass, casings, boxes, and cases.
3. Concealed Weapons Permit(s).
4. Records, documents, notes, receipts, ledgers, invoices, indicia, or photographs showing the acquisition or sale of any firearms and firearm parts.
5. Receipts, bank account records, buyer or seller lists, money transfer records, agreements for storage facilities, records of mail service, ledgers, and notebooks showing the acquisition and/or disposition of firearms and firearm parts.
6. Books, records, receipts, notes, ledgers, personal checks and other papers relating to the transportation, ordering, and purchase of firearms, firearm accessories, or ammunition.
7. Ledgers, customer lists, contact lists, inventory lists, vendor lists, or any notes containing the individual names of such persons, telephone numbers or addresses of such persons.
8. Bank documents and records, financial documents and records, and any records and documents relating to any bank or financial transactions, including: correspondence, signature cards and applications for all credit card accounts, investment accounts, and retirement accounts; copies of monthly, quarterly, yearly or periodic account statements; pre-paid credit/debit cards; money wrappers; copies of check journals, check ledgers, checkbooks, check registers, deposit tickets, deposit items, credit memos, debit memos, canceled checks, loan applications, financial statements,

mortgage or promissory notes; copies of loan ledger accounts; copies of annual loan statements; application for bank drafts, cashier's checks, and foreign drafts; and records relating to employment, wages earned and paid, business income earned, and other compensation records.

9. Records indicating occupancy, residency, or rental of the search location, including rental or lease agreements, and keys.
10. Records pertaining to the rental of self-storage units, post office boxes, or mailboxes.
11. Electronic equipment, including cellular telephones, computers, disks, thumb drives, and any media storage device, GPS devices and their memory, and related manuals used to generate, transfer, count, record or store the information described in this Attachment B. For any computer or electronic storage medium whose seizure is otherwise authorized by this warrant, and any computer or electronic storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, the "Electronic Storage Device"), this warrant also authorizes the seizure of the following:
 - a. Evidence of who used, owned, or controlled the Electronic Storage Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, and browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. Call details including call history, duration of calls, text messages, and text message history;
 - c. Electronic correspondence and communications stored on, or accessed through, the Electronic Storage Device relating to the procurement of export-controlled items, to include e-mails and attached files, text messages, any Short Message Service messages (SMS), Instant Messages (IM), Multimedia Message Service messages, or similar text or electronic messages made

through additional applications from which communication can be made, and instant messaging logs;

- d. Contact lists stored on or accessed through the Electronic Storage Device, to include telephone and e-mail contact names, telephone numbers, addresses, and e-mail addresses;
- e. Evidence of software that would allow others to control the Electronic Storage Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- f. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- g. Evidence indicating how and when the Electronic Storage Device was accessed or used to determine the chronological context of Electronic Storage Device access, use, and events relating to the crime under investigation and to the user of the Electronic Storage Device;
- h. Evidence of the attachment to the Electronic Storage Device of other storage devices or similar containers for electronic evidence;
- i. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Electronic Storage Device;
- j. Evidence of the times the Electronic Storage Device was used;
- k. Passwords, encryption keys, and other access devices that may be necessary to access the Electronic Storage Device;
- l. Documentation and manuals that may be necessary to access the Electronic Storage Device or conduct an examination of the Electronic Storage Device;
- m. Any records of or information about Internet Protocol addresses used

- by the Electronic Storage Device;
 - n. Contextual information necessary to understand the evidence described in this Attachment B; and,
 - o. Any peripheral equipment used to facilitate the transmission, creation, display, encoding or storage of records, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners.
12. Items used for identification, including identification cards under fictitious names, and any other type of false identifying documents.

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Katherine Rottman, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. This affidavit is submitted in support of an application for a warrant to search the following property for evidence of violations of 18 U.S.C. § 924(a)(1)(A), False Statement in the Purchase of a Firearm:.

- a. 611 W Indian School Rd Unit 323, Phoenix, Arizona 85013 (**Subject Premises A-1**), further described in Attachment A-1; and,
- b. a 2015 silver Mercedes Benz, Class C Sedan, bearing California license plate 8XQZ564 and VIN ending in 88618 (**Subject Premises A-2**), further described in Attachment A-2.

2. I am a Special Agent (SA) with the Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF) and have been since June 2020. I am graduate of the Federal Law Enforcement Training Center, Criminal Investigator Training Program. and a graduate of the ATF National Academy Special Agent Basic Training programs in Glynco, Georgia. I am empowered by law to conduct investigations of and make arrests for offenses enumerated in Section 2516 of Title 18, United States Code.

3. My training in law enforcement includes agency specific training in all aspects of conducting federal criminal investigations, including the planning, preparation, and execution of search warrants. I am an “investigative or law enforcement officer of the United States” within the meaning of Title 18, U.S.C. § 2510(7), authorized to conduct investigations into alleged violations of federal law.

4. Through my training and experience, I know that it is a violation of federal law for any person who knowingly makes a false statement or representation during the purchase of a firearm with respect to the information required by federal law to be kept in the records of an FFL according to 18 U.S.C. § 924(a)(1)(A).

5. This affidavit is intended to show that there is sufficient probable cause for the requested search warrant and does not purport to set forth all my knowledge of or investigation into this matter. The statements set forth in this affidavit are based upon my investigation to date, my experience, my training, and other reliable sources of information relative to this investigation.

PROBABLE CAUSE

5. As of November of 2021, ATF has been investigating the activities of Andrew MOON and Manuel SALAZAR regarding violations of 18 U.S.C. § 924(a)(1)(A), knowingly making a false statement or representation during the purchase of a firearm with respect to the records required by federal law to be kept by an FFL.

6. SALAZAR and MOON purchased over 100 firearms from multiple FFLs between July 16, 2021 and March 22, 2022. All purchases were conducted from FFLs in the greater Phoenix area. ATF has reviewed ATF Form 4473s for the following transactions where SALAZAR and MOON both provided a false residence address of 8650 S 29th Ave., Laveen, Arizona. ATF is in the process of obtaining all other ATF Form 4473's for each transaction.

7. ATF estimates that SALAZAR and MOON paid approximately \$100,000 for these firearm purchases.

8. ATF does not know of any firearm recoveries.

9. On December 9, 2021, ATF SAs Nathaniel Merritt and Hannah Carroll attempted to contact SALAZAR and MOON at 8650 S 29th Ave Laveen, Arizona, as that is the address they both listed repeatedly on ATF Form 4473s. SAs interviewed the resident at the time of 8650 S 29th Ave., Laveen, Arizona: Shawni Soto. Soto stated that she had lived at the address for "two weeks and moved in about two days before Thanksgiving" and had not ever seen SALAZAR or MOON. When shown photos of SALAZAR and MOON, she did not recognize either one.

10. SAs Merritt and Carroll also spoke with the property owner for 8650 S 29th Ave., Laveen, Arizona: Misty LaSalvia. LaSalvia stated that she did not know SALAZAR

or MOON and did not recognize their names. LaSalvia was shown photos of MOON and SALAZAR, and she did not recognize them as tenants. LaSalvia did state that she evicted a tenant who was allowing transients to live in the backyard of the residence approximately 6 months prior.

11. Between June and December 2021, after the eviction and prior to Shawni Soto living there, LaSalvia was leasing the property to migrant workers from Mexico. Photos of SALAZAR and MOON were shown to her, and she again stated that MOON and SALAZAR did not live at the residence during this time.

12. On March 23rd, 2022, SA Holden knocked on MOON's purported residence at 3602 Patio Place, Los Angeles, California. No one answered the door.

13. SA Holden knocked on the residence of 3604 Patio Pl., Los Angeles, California, and spoke with MOON's neighbor, who remained anonymous. The following is a summary of the information provided by MOON's neighbor:

- a. MOON was currently not home but typically arrives home between 4–6 p.m.;
- b. MOON lives at 3602 Patio Place, with his uncle, whom the only knew by his nickname;
- c. MOON was already living at 3602 Patio Place when the neighbor moved in approximately three years ago;
- d. The neighbor does not have a close relationship with MOON;

14. SA Holden and SA Lozano knocked on the residence of 3612 Patio Place, Los Angeles, California, and spoke with SALAZAR's brother, Adrian. The following is a summary of the information provided by Adrian:

- a. Adrian stated SALAZAR lives at the residence but was not home;
- b. Adrian stated is typically gone for approximately one to two weeks at a time and then will return home for approximately one or two nights;
- c. Adrian stated that he did not where SALAZAR goes when he is away for the long periods of time;

d. Adrian provided SAs with the telephone number (XXX-XXX-7697) as a way to contact SALAZAR.

15. Of the firearms purchased between July 16, 2021 and March 7, 2022 by MOON, nine were Glock 19 9mm handguns. Three of the purchased firearms were Glock 17 9mm handguns.

16. According to law enforcement databases, MOON has a silver Mercedes bearing CA plate 8XQZ564 (**Subject Premises A-2**) registered to him at an address of 3602 Patio Pl., Los Angeles, CA. The registration is valid from 6/26/21 to 6/26/22.

17. SALAZAR does not have a vehicle registered to him in the state of Arizona or California.

18. As of this writing, SA Rottman does not possess all ATF Form 4473s for all of MOON and SALAZAR's known firearm purchases. On March 23, 2022, SA Rottman received the following 4473s:

a. On 01/10/2022, MOON purchased two firearms from Refiners Firearms in Anthem, Arizona, and provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473;

b. On 01/10/2022, SALAZAR purchased one firearm from Refiners Firearms in Anthem, Arizona, and provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473;

c. On 01/10/2022 MOON purchased one firearm from Ammo AZ in Phoenix, Arizona, and provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473;

d. On 1/20/22, SALAZAR purchased one firearm from Ammo AZ in Phoenix, Arizona, and provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473;

e. On 1/20/22, MOON purchased one firearm from Ammo AZ in Phoenix, Arizona, and provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473;

f. On 1/21/22, MOON purchased two firearms from Ammo AZ in Phoenix, Arizona, and provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473;

g. On 2/14/2022, MOON purchased one firearm from Ammo AZ in Phoenix, Arizona, and provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473;

h. On 02/15/2022, SALAZAR purchased one firearm from Ammo AZ in Phoenix, Arizona, and provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473;

i. On 02/23/2022, SALAZAR attempted to purchase one firearm from Ammo AZ in Phoenix, Arizona, and provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473; this purchase was not completed because SALAZAR was denied by the NICS background check.

j. On 02/23/2022, MOON purchased one firearm from Ammo AZ in Phoenix, Arizona, and provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473;

k. On 03/7/2022, SALAZAR purchased two firearms from Ammo AZ in Phoenix, Arizona, and provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473;

l. On 02/7/2022, MOON purchased two firearms from Ammo AZ in Phoenix, Arizona, and provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473;

m. On 03/22/2022, MOON purchased two firearms from Ammo AZ in Phoenix, Arizona, and provided a residence address of 611 W Indian School Rd #323 Phoenix, Arizona (**Subject Premises A-1**);

n. On 03/22/2022, SALAZAR attempted to purchase two firearms from Ammo AZ in Phoenix, Arizona, and provided a residence address of 611 W Indian School Rd #323 Phoenix, Arizona (**Subject Premises A-1**); this purchase was not

completed because SALAZAR was delayed by the NICS background check; the FFL reported to SAs that SALAZAR nevertheless chose to prepay for the firearms.

19. On March 22, 2021, SA Rottman received a phone call from GCS Armory, a home-based FFL located in Surprise, Arizona. GCS Armory stated that two males, MOON and SALAZAR, had come in several times to purchase firearms together. He stated that MOON and SALAZAR claimed to be cousins. According to the owner, MOON and SALAZAR come in, each purchase one Glock 45, 19, or 17 each, pay in cash, and leave. MOON and SALAZAR have done this several times. The owner of GCS Armory told SA Rottman that he found their behavior odd, so he called of friend of his who also operates a home-based FFL, Desert Ballistics, located in Surprise, Arizona. The owner of Desert Ballistics stated that MOON and SALAZAR have done the same thing at his FFL multiple times.

20. SA Rottman requested the 4473s from GCS Armory and Desert Ballistics. On February 15, and March 7, 2022, MOON filled out an ATF form 4473 to purchase a Glock 19x 9mm handgun and Glock 17 9mm handgun at GCS Armory. MOON stated on the form on both occasions that his current address was 8650 S 29th Ave., Laveen, Arizona. On the same dates at GCS Armory, SALAZAR purchased a Glock 17 Gen 5 and an FN America 57, respectively. On both occasions, SALAZAR provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473s.

21. On 1/20/22, 2/14/22, and 3/7/22, MOON purchased a Glock 19x, a Glock 19 and a Glock 45, respectively, from Desert Ballistics. On each occasion, MOON provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473s.

22. On 2/14/22 and 3/7/22, SALAZAR purchased a Glock 17 and a Glock 19x, respectively, from Desert Ballistics. On both occasions, SALAZAR provided a residence address of 8650 S 29th Ave., Laveen, Arizona, on the ATF Form 4473s.

23. On 3/22/22, MOON attempted to purchase a Glock 19 Gen 5 from GCS Armory. He arrived inside the FFL alone, but the owner noticed that SALAZAR was outside, in **Subject Premises A-2**. On this occasion, MOON provided a residence address

of 611 W Indian School Rd #323 Phoenix, Arizona (**Subject Premises A-1**), on the ATF Form 4473. MOON was delayed for this transaction by the NICS background check.

24. When GCS Armory delayed MOON, MOON stated that he had been to several other FFLs earlier that day and had even purchased a Barrett .50 caliber firearm with no issue. NICS flags show that MOON went to seven FFLS on 3/22/22.

25. Between 12/23/21 and 03/08/22, the Drug Enforcement Agency Special Intelligence Link (DEASIL), a law enforcement license plate reading system, shows six sightings of **Subject Premises A-2** traveling northbound on US Highway 93 (Kingman), which leads to Las Vegas.

26. The **Subject Premises A-2**'s license plate was also run through Vigilant LPR, another law enforcement license plate reader for metropolitan areas. There was a Vigilant sighting of **Subject Premises A-2** on 02/11/22 at 2101 hours (PST) just north of Tijuana, Mexico.

27. **Subject Premises A-2** has a total of 60 encounters (mostly at San Ysidro Point of Entry in CA) between 08/08/21 and 03/20/22. Several of the crossings show inbound/outbound on the same day. Both MOON and SALAZAR have multiple border crossings together in **Subject Premises A-2**.

28. On 07/29/20, MOON was apprehended with \$18,100 of undeclared currency traveling from the United States into Mexico in **Subject Premises A-2**.

29. On March 23, 2022, ATF agents went to **Subject Premises A-1**, the address of which SALAZAR and MOON recently used on ATF forms 4773 to purchase firearms. The address is a Budget Suites of America described as an extended stay with weekly rates. SA Rottman observed **Subject Premises A-2** parked in the parking lot and initiated surveillance. TFO Fulton spoke to the management of **Subject Premises A-1**, who advised that MOON and SALAZAR initiated their extended stay on March 22, 2022, in unit 323. Fulton was provided with the "Move in Form" where the primary tenant was listed as MOON and the secondary tenant was listed as SALAZAR. They listed **Subject Premises A-2** as their vehicle.

30. Under employer, MOON listed “self” and listed an address on Patio Place, Los Angeles California. In addition, the leasing office of **Subject Premises A-1** told TFO Fulton that SALAZAR and MOON had paid in advance for a week-long stay, which is the minimum.

31. SAs initiated surveillance on **Subject Premises A-1** and **A-2**. At approximately 1010 hours, SA Morales observed subjects fitting the description of MOON and SALAZAR exit **Subject Premises A-1** and walk down the stairs carrying a large black gun case. The gun case fit the description of a .50 caliber gun case and both subjects were seen putting the gun case in the back of **Subject Premises A-2**. Both subjects returned to **Subject Premises A-1** and moments later were seen carrying a large plastic bag that was also placed in **Subject Premises A-2**. The subjects returned to **Subject Premises A-1** a third time and came out with duffle bags and backpacks.

32. Moments later, ATF agents approached MOON and SALAZAR and detained both subjects for suspicion of making false statements in the purchase of firearms.

33. SA Morales spoke to MOON after he was Mirandized. When asked where he was currently living, MOON stated that they had just moved into **Subject Premises A-1** two days prior. When asked where he lived prior to that, MOON stated that he had lived in Laveen since July 2021, but did not know what his address was. He stated that he grew up in Los Angeles, California, and provided the same address that he put on the **Subject Premises A-1** leasing form. MOON stated that he had paid for a whole month and planned on staying at **Subject Premises A-1** longer. MOON provided his cellular telephone number and shortly thereafter requested to speak to his attorney. SAs terminated the interview.

34. SA Gonzalez then contacted the leasing office at **Subject Premises A-1**. They advised that MOON did pay for a month-long stay. SAs obtained cellular telephones from MOON and SALAZAR’s persons. Both subjects were found to possess two phones on their persons.

35. On March 22, 2022, GCS Armory informed SAs that every time MOON and SALAZAR visited his FFL, they have been driving the **Subject Premises A-2**.

36. On March 22, 2022, GCS Armory took the following photo of the **Subject Premises A-2** at the FFL:



37. On March 23, 2022, during contact with ATF agents, MOON stated that the **Subject Premises A-2** belonged to him.

38. Neither MOON nor SALAZAR have an employment history or income in the last four years in the state of Arizona. According to GCS Armory and Desert Ballistics, MOON and SALAZAR consistently paid in cash.

39. Based on my training and experience and based on the high number of border crossings, MOON and SALAZAR's behavior is indicative of firearms trafficking and illegal exportation of firearms to Mexico. In addition, they are utilizing an address which they do not reside at to complete ATF Form 4773s. Per the property owner in Laveen, neither SALAZAR nor MOON live or have ever lived at the Laveen address. SALAZAR'S family and MOON'S neighbors have all stated that MOON and SALAZAR currently reside in the state of California.

TRAINING AND EXPERIENCE – DIGITAL DEVICES/MEDIA

40. Through my training and experience as an ATF SA, I have learned that many people keep records of their firearms, including digital photographs or recordings of

themselves possessing or using firearms on their digital devices. It has been my experience that unlicensed dealers of firearms who purchase firearms illegally will keep the contact information of the individual to whom he or she sells firearms for future sales and/or sales referrals from established customers. I know that much correspondence is via digital devices. I know that much correspondence between persons buying and selling firearms often occurs by e-mail or text message sent to and from digital devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price.

41. Therefore, based on my experience, I believe that it is probable that digital devices may contain text messages or e-mails between MOON, SALAZR, and other individuals discussing the possession, sale or transfer of firearms. In my experience it is common for straw purchasers of firearms to have photographs of firearms they or other individuals possess on their digital devices as they frequently send these photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms. I also know that people keep receipts from sales and purchases of items related to firearms possession, including ammunition, holsters, etc.

42. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a

premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed

via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated

with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

43. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

ITEMS TO BE SEIZED

44. Based upon the facts contained in this Affidavit, your Affiant submits there is probable cause to believe that the items listed in Attachment B will be found at **Subject Premises A-1 and A-2**.

45. Based on my training, education, and experience, and discussions with other trained law enforcement personnel, along with information provided by sources of information and confidential sources, your Affiant knows the following:

a. Firearm traffickers often keep large amounts of United States currency on hand in order to maintain and finance their ongoing trafficking activities. Traffickers commonly maintain such currency where they have ready access to it, such as in their homes and vehicles. It is also common for traffickers to possess trafficking proceeds and items purchased with proceeds in their homes and vehicles. Thus, it is common for currency, expensive jewelry, precious metals, or financial instruments to be found in the possession of firearm traffickers.

b. Traffickers often maintain paper records of their firearms trafficking and money laundering activities. Your Affiant knows that such records are commonly maintained for long periods of time and therefore are likely to be found at the **Subject Premises**.

c. Firearm traffickers commonly use computers, cellular telephones, and other electronic devices to communicate with other drug traffickers and customers about drug-related activities through the use of telephone calls, text messages, email, chat rooms, social media, and other internet- and application-based communication forums. Moreover, firearm traffickers commonly use other capabilities of computers and electronic devices to further their drug trafficking and money laundering activities. Therefore, evidence related to firearm trafficking activity and money laundering activity is likely to be found on electronic storage media found at the **Subject Premises**, as further described below.

46. In addition to items which may constitute evidence, fruits and/or instrumentalities of the crimes set forth in this Affidavit, your Affiant also requests

permission to seize any articles tending to establish the identity of persons who have dominion and control over the **Subject Premises**, including rent receipts, utility bills, telephone bills, addressed mail, personal identification, keys, purchase receipts, sale receipts, photographs, vehicle pink slips, and vehicle registration.

DIGITAL EVIDENCE STORED WITHIN ELECTRONIC STORAGE MEDIA

47. As described in Attachment B, this application seeks permission to search for records that might be found in or on the **Subject Premises**, in whatever form they are found, including data stored on a cellular telephone, hereafter referred to as “electronic storage media”). Thus, the warrant applied for would authorize the seizure of all electronic storage media found in or on the **Subject Premises** and, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

48. *Probable cause.* Your Affiant submits that if electronic storage media are found in or on the **Subject Premises**, there is probable cause to believe records and information relevant to the criminal violations set forth in this Affidavit will be stored on such media, for at least the following reasons:

a. Your Affiant knows that when an individual uses certain electronic storage media, the electronic storage media may serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage media is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic storage media is also likely to be a storage medium for evidence of crime. From my training and experience, your Affiant believes that electronic storage media used to commit a crime of this type may contain: data that is evidence of how the electronic storage media was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

b. Based on my knowledge, training, and experience, your Affiant knows that electronic storage media contain electronically stored data, including, but not limited to, records related to communications made to or from the electronic storage media, such as the associated telephone numbers or account identifiers, the dates and times of the communications, and the content of stored text messages, e-mails, and other communications; names and telephone numbers stored in electronic “address books;” photographs, videos, and audio files; stored dates, appointments, and other information on personal calendars; notes, documents, or text files; information that has been accessed and downloaded from the Internet; and global positioning system (“GPS”) information.

c. Based on my knowledge, training, and experience, your Affiant knows that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on an electronic storage medium, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

49. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the electronic storage media were used, the purpose of their use, who used

them, and when. There is probable cause to believe that this forensic electronic evidence will be found on any electronic storage media located in or on the **Subject Premises** because:

a. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. File systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within electronic storage medium (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware

detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the owner. Further, activity on an electronic storage medium can indicate how and when the storage medium was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on an electronic storage medium may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the existence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera) not previously identified. The geographic and timeline information described herein may either inculcate or exculpate the user of the electronic storage medium. Last, information stored within an electronic storage medium may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within a computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic storage medium evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on one electronic storage medium is evidence may depend on other information stored on that or other storage media and the application of knowledge about how electronic storage media behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how an electronic storage medium was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

50. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on electronic storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine electronic storage media to obtain evidence. Electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the electronic storage media off-site and reviewing it in a controlled environment allows for a thorough examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of electronic storage media formats that may require off-site reviewing with specialized forensic tools.

51. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your Affiant is applying for would permit seizing, imaging, or otherwise copying electronic storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might

expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

52. Based upon my training and experience, and the facts set forth herein, I submit that there is probable cause to believe that the items described in Attachment B are evidence of violations of 18 U.S.C. § 924(a)(1)(A), knowingly making a false statement or representation in the purchase of a firearm; will be found in the property set forth in Attachment A.

**KATHERINE
ROTTMAN** Digitally signed by
KATHERINE ROTTMAN
Date: 2022.03.23 18:14:35
-07'00'

KATHERINE A ROTTMAN, Special Agent
Bureau of Alcohol, Tobacco, Firearms &
Explosives

Sworn to telephonically before me this 23rd day of March 2022.



HONORABLE EILEEN S. WILLETT
United States Magistrate Judge